KYND

Cyber risks in the legal sector

If there's one thing that law firms do not have immunity from, it's cybercrime – in fact, even the General Council of the Bar had to have its systems taken offline earlier this year, to protect itself from a vicious cyber attack. Irrespective of size, law firms are judged to be a good target by cybercriminals, due to the large amounts of client money, data and sensitive information they hold. Sensitive client data is highly valuable, as it often includes personal, business and commercial information such as medical records, government secrets, all of which can be used as blackmail or employed in targeted phishing attacks.

The financial and reputational impact of cyber attacks on law firms is also significant. In March of this year, the landmark decision was made by the ICO to fine law firm Tuckers Solicitors the hefty fee of £98,000[1] – not for falling victim to the cyber attack that took place in 2020, but for failing to securely process the personal data of their clients. This just demonstrates the need to adequately protect the sensitive data that law firms deal with on a daily basis!

The costs arising from an attack itself can be massive, but the losses from fines, reputational damage, and difficulty in regaining client trust, can be devastating. The cyber threat to the legal sector is a significant trial for organisations, and the number of reported incidents has grown over the last few years. GDPR adds a further regulatory burden with stringent requirements for collating, storing and processing data as well as reporting data breaches.

KYND is taking the case! We object to cybercriminals taking advantage of vulnerabilities, and we are here to help the legal sector defend itself with our proactive approach to managing cyber risks.

Business exposure and implications

Access to confidential and sensitive client information

Lawyers hold sensitive client information, handle significant funds, and are a key enabler in commercial and business transactions. The loss of client information can have a devastating impact on a sector that has confidentiality at the heart of its business. Law firms with politically or commercially sensitive clients are likely to be at a higher risk of data breach than a local high street firm.

Reputational damage

Law firms are entrusted by their clients to keep their information confidential and secure. A cyber attack and a potential breach of this confidentiality could seriously harm a firm's hard-won reputation. Something that may not be easy to recover from.

Increased reliance on technology

The move to offer legal services digitally will not only provide new opportunities but also further avenues for malicious cyber exploitation.

Supply chain exposure

A law firm's supply chain can be numerous and diverse, and it can be compromised in various ways. By far the greatest issue is a third party supplier failing to adequately secure the systems that hold clients' sensitive data. The increasing use of digital technologies to deliver legal services will likely offer further avenues for exploitation.

Key industry statistics

23,000

the number of people whose personal information was compromised in a recent law firm's data breach[2]

60%

is the rise in attacks against businesses in the law sector in the last two years[3]

£4m

is the amount of client money stolen from 23 of the law firms targeted in a cyber attack in 2020[4]

73%

of the UK top 100 law firms have been a target of a cyber attack[5]

What types of risks exist?

There is a variety of different threats that could impact the legal sector, but the most common include:

Phishing
Malicious emails designed to look like genuine emails which encourage employees to click – infecting their computers or stealing passwords in the process.

Viruses
Code which infects computer systems, corrupting or deleting data.

Hacking
An individual or group attempting to gain access to company systems with the intent to steal or destroy data.

Ransomware
A malicious programme which locks access to company files and data until a ransom payment is made, after which time access may be restored.

KYND

KYND's analysis of key cyber risks of the top* 200 UK legal companies
*by turnover

Email Spoofing

91.0% of companies were vulnerable to having their email addresses spoofed.

Vulnerable Services

80.5% of companies were running at least one service, such as an email server or web server, with a well-known vulnerability to cyber attack.

Out of Date Software

21.0% of companies had at least one service that was using software which was out of date, no longer supported and vulnerable to cyber attack.

Certificate Issues

23.0% of companies had at least one security certificate which had expired, been revoked or distrusted.

Case Study

Type
Phishing attack on mid-sized law firm with multi-million pound turnover.

Scenario
A senior partner posted on social media with full details about a business trip to Barcelona (flight, meeting plans, weather etc) and criminals used this to initiate a phishing attack. An accounts clerk at the company then received an email from an account spoofing the senior partner's email address, instructing her to pay an invoice and imploring confidentiality.

Sting
The criminals also knew that the accounts team were tied-up in installing a new accounting package and training on the new system, as a staff member had mentioned it on Facebook. It was at this time that the criminals convinced the clerk to make an authorised payment of £35,000. The firm only realised it had fallen victim to phishing when another senior partner later queried the transaction.

Investigation
The scam was reported to local law enforcement and the firm attempted to recover the funds from the recipient bank, but all of the money had been moved out of the fraudulent account and the prospects of a successful recovery were deemed to be remote.

Conclusion
The company did have cybercrime cover on their cyber insurance policy and were able to recover cost in full.

How KYND can help

- With just a website name, KYND reveals your organisation's cyber risks
- Instantly KYND lets you know if your emails are spoofable or if you're vulnerable to a ransomware attack
- KYND provides clear and easy recommendations without using technical jargon
- KYND continuously monitors and alerts you instantly if any new cyber risks are found

Get in touch
broker@kynd.io
www.kynd.io

References:
[1] https://www.solicitorsjournal.com/sjet/bc/suckers-solicitors-fined-59000-by-ico-over-data-breach. 2022. Solicitors Journal.
[2] https://www.law.com/thelegalintelligencer/2022/05/13/law-firm-cyber-breach-may-impact-22k-including-financial-institution-clients-customers/?slreturn=20220701101433. 2022. ALM Global
[3] https://easylaptopdeals.com/the-key-cybersecurity-threats-facing-law-firms-in-2022/. 2022. Law Pain and Simple
[4] https://www.lawsociety.org.uk/topics/cybersecurity/a-candid-conversation-on-cyber. 2021. The Law Society
[5] https://uhy.co.uk/cyber-attacks-law-firms-increasing-firms-secure/. 2021. Cyber